CLIENT ALERT

EU Data Protection Authorities Finds Transfer of Financial Data by SWIFT to U.S. Department of Treasury Illegal

Dec.18.2006

On November 22, 2006, the European Privacy Watchdog, known as the EU Working Party, issued a lengthy Opinion on the transfer of personal data to the US Department of Treasury ("Treasury") by SWIFT. The Working Party Opinion, which parallels the Belgian Data Protection Authority's ("DPA's") findings from September 2006, concludes that the transfer of banking records to Treasury constitutes a violation of the EU data protection laws by SWIFT and the financial institutions participating in the SWIFT system.

SWIFT is the backbone of an international inter-bank network that serves 7,800 financial institutions worldwide and is headquartered in Belgium. In June 2006, it became public that SWIFT had disclosed personal information on financial transactions in response to subpoenas issued by Treasury. Those subpoenas, issued after the September 11 terrorist attacks, sought information regarding potential terrorist financing, and Treasury was given unlimited access to certain files under a “black box” data storage system.

The Working Party opined that:

- SWIFT and the financial institutions are jointly responsible to process financial transaction information in compliance with the EU Directive Data Protection Directive 95/46 (the Directive).

- SWIFT has put EU citizens' privacy at risk by (i) setting up a mirror server in the US to store data of all financial transactions; and (ii) agreeing to a “massive data transfer” that provides Treasury unlimited and uncontrolled access to banking records.

- SWIFT should assume full responsibility as a "data controller" under the EU Data Protection Directive (which includes providing notice to individuals, obtaining a legal basis to transfer personal data outside the EU, etc.).

- The financial institutions have an affirmative obligation to inform themselves about “the different payment systems" utilized by their subcontractors and the "technical and legal characteristics and risks” associated with each. This requirement would seem to impose something close to a strict liability regime as to the privacy implications resulting from the use of information systems by the institutions, their vendors and other contractors.

- Taking a position that has sweeping implications, the Working Party found that SWIFT could not rely on Treasury subpoenas to justify the disclosure of banking records to Treasury since “[a]n obligation imposed by a foreign legal statute or regulation may not qualify as a legal obligation by virtue of which data processing in the EU would be made

legitimate." The Working Party did recognize that "SWIFT has a legitimate interest in complying with the subpoenas under US law," but concluded that in this specific case, SWIFT did not appropriately balance individuals' data protection rights with its legitimate interest to comply with the subpoenas.

- SWIFT cannot rely on the data transfer exemptions set forth in Article 26 of the Directive to transfer the banking records to the US.

With respect to the transatlantic export of banking records to the US, SWIFT tried to legitimize such an export on the legal basis that it "is necessary or legally required on important public interest grounds, or for the establishment, exercise or defense of legal claims" (Article 26 (1)(d) of the Directive). SWIFT stressed that the transfer and disclosure of personal data to Treasury must be permitted because the processing of such information to fight terror must be considered an important public interest ground. The Working Party rejected this argument, stating that "only important public interests identified as such by the national legislation applicable to data controllers established in the EU are valid in this connection." The Opinion does not preclude companies from asserting that this exemption permits the transfer of personal data to the US to comply with a court order or a subpoena in the context of pending litigation, but it does confirm that the Data Protection Authorities interpret Article 26 data transfer exemptions restrictively.

Finally, some recent articles in the Belgian press indicate that the Belgian Public Prosecutor has also investigated SWIFT's operations, but appears to have concluded that SWIFT did not commit a criminal offense in connection with this transfer of data. It is not entirely clear whether the Belgian or European authorities will take any further action against SWIFT (and/or the financial institutions).

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Kris D. Meade
Partner – Washington, D.C.
Phone: +1 202.624.2854
Email: kmeade@crowell.com